

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 INFORMATION ASSOCIATED WITH
 ashwimvijayrao@gmail.com THAT IS STORED AT
 PREMISES CONTROLLED BY GOOGLE INC.

Case No.

18MJ340-1

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
 Email account of ashwimvijayrao@gmail.com located at Google Incorporated, 1600 Amphitheatre Way, Mountain View, California 94043

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):
 email account: ashwimvijayrao@gmail.com

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

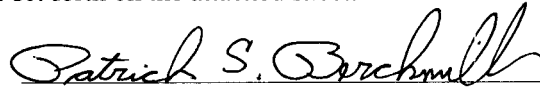
Code Section
 18 U.S.C. § 1343
 18 U.S.C. § 1349

Fraud by Wire, Radio or Television
 Attempt and conspiracy

Offense Description

The application is based on these facts:
 See attached.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Applicant's signature

Patrick S. Berckmiller Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

11/20/18 9:05 AM


 Judge's signature

City and state: DURHAM, NC

HON. JOE L. WEBSTER, U.S. MAGISTRATE JUDGE

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH
OF INFORMATION ASSOCIATED
WITH ashwimvijayrao@gmail.com
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE INC.

Case No. 18MJ340-1

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

1. I, Patrick S. Berckmiller, affiant herein, being first duly sworn,
hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

2. I am a Special Agent of the Federal Bureau of Investigation (FBI) and has been so employed since November 1998. Since April 2016, affiant has been assigned to investigate cyber-related crimes to include fraud and related activity in connection with computers. From March 1999 until April 2016, affiant was assigned to investigate foreign counterintelligence matters and theft of trade secrets crimes. Affiant received training from the FBI regarding cyber crimes, foreign counterintelligence and theft of trade secrets, and has previously been involved in investigations involving espionage, export violations, bank robbery, kidnapping, fugitives from justice, white collar crimes and computer crimes involving the theft of proprietary data. Most

recently, I have been involved in an investigation regarding a Business Email Compromise (BEC). As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343, Fraud by Wire, Radio or Television, and 18 U.S.C. § 1349, Attempt and conspiracy have been committed by Lamar Rhashad MURRIELL and James RAGLAND. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

5. I make this affidavit in support of an application for a search warrant for information associated with one e-mail account that is stored at premises controlled by Google Inc., an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information

to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google Inc. to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. *See* 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the United States District Court for the Middle District of North Carolina is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. This affidavit proceeds as follows. In this section, I outline the factual allegations in support of a warrant to search one email account.

Business Email Compromise #1

8. In June 2018, Federal Bureau of Investigation Special Agent Patrick Berckmiller learned of a Business Email Compromise (abbreviated BEC, a

sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments). In February 2018, Sari Gallegos ("VICTIM 1") was purchasing a home at 8140 San Miguel Avenue, South Gate California. Gallegos received wiring instructions for the down payment of her home from her loan officer, Steve Racijs. However the email address where the instructions came from was frontdesk_add@comcast.net. The email was ostensibly from Steve Racijs and provided wiring instructions for the down payment for this property. The fraudulent wiring instructions sent to Gallegos at her email address of Gallegos.sari@yahoo.com caused her to wire \$56,593.90 on February 6, 2018, into Bank of America account number 237037782397.

9. This Bank of America account was opened on December 29, 2017, under the name of Murrays International Consulting, owned by Lamar Rhashad MURRIELL, DOB: April 30, 1987, address: 5107 Twelvepole Drive, Raleigh, NC 27616-5877. MURRIELL is the only person listed on this account and is identified as "President" of this company on the Bank of America Business Signature Card, dated December 29, 2017. MURRIELL provided a North Carolina driver's license, number 20594244, as identification to Bank of America. The investigation determined that this Bank of America account had two withdrawals made by two checks on

February 7, 2018. These two cashier's checks from Bank of America were made payable to Lamar Rhashad MURRIELL for \$15,541.00 and to James RAGLAND for \$32,885.00.

10. James RAGLAND, DOB July 31, 1991, is the only authorized signer for Woodforest National Bank Business Simple Checking Account number 1827001783 (under the business name of Throne Management Group LLC.) RAGLAND provided the email address of jay_rag@yahoo.com and identified himself as the "President" of Throne Management Group LLC. On February 7, 2018, RAGLAND made three deposits to this bank account, in the amounts of \$33,275.00, \$75.00 and \$1,800.00, for a total deposit amount of \$35,150.00. RAGLAND'S three deposits on February 8, 2018, included the check from the Murrays International Consulting account for \$32,885.00, which originated from the fraudulent wire transfer from VICTIM 1.

11. On February 8, 2018, James RAGLAND wired \$22,000.00 from Woodforest National Bank Account number 1827001783 to State Employee Credit Union account number 08644583711 (beneficiary: James RAGLAND). On February 8, 2018, RAGLAND also made three withdrawals from the Woodforest National Bank Account in the amounts of \$2,000.00, \$3,036.00 and \$1,000.00. The total withdrawals made by RAGLAND on February 8, 2018 were \$28,036.00.

12. The remaining funds from the fraudulent wire transfer totaled \$8,167.14, and were used by MURRIELL's debit card. The purchases included payments on a car loan and car insurance in the name of MURRIELL. Additionally, MURRIELL purchased two handguns in his name along with ammunition and a holster. MURRIELL also made purchases for shoes, a laptop computer and other electronics. MURRIELL closed the Murrays International Consulting account at Bank of America on February 14, 2018.

Business Email Compromise #2

13. On or about March 23, 2018, Evergreen Settlement, 8923 Shady Grove Court, Gaithersburg, Maryland 20877, served as the settlement company in a real estate transaction involving an owner and seller of a property located at 8603 Enoch Pratt Drive, Ellicott City, Maryland 21043. Evergreen Settlement received fraudulent wiring instructions from email address ashwimvijayrao@gmail.com, directing \$95,282.88 to be wired to Wells Fargo Bank account 9869840554. The beneficiary was intended to be Ashwin Rao (VICTIM 2), but the fraudulent instructions changed the beneficiary to "Ashwin Rao Precision". Wells Fargo Bank account number 9869840554 is in the name of "Precision Trucking and Transport Inc." with an additional account customer identified as Lamar Rhashad MURRIELL.

The bank account application states that it was established on March 5, 2018, with annual gross sales of \$250,000.00, with one location and one employee. The industry is identified as "Transportation and Warehousing" and the description of the business: "TRUCK DRIVERS". The account was opened on March 16, 2018, with the listed address being 3737 Glenwood Avenue, Suite 100, Raleigh, North Carolina 27612. That is an address for a Regus business location, which rents office space, virtual offices, co-working spaces and meeting rooms. The April 2018 statement for this bank account lists 5107 Twelvepole Drive, Raleigh, NC 27616-5877, the home address for Lamar Rhashad MURRIELL. Evergreen identified the fraudulent instructions and did not wire any funds. This account was closed on June 22, 2018.

Business Email Compromise #3

14. On December 7, 2017, Westar Escrow, Incorporated, of San Diego, California, served as a party in a real estate transaction involving an owner and a seller of a property. The beneficiary was listed as Michael and Lydia Wisz (VICTIM 3). Westar received fraudulent wiring instructions from email address supportcentr@comcast.net directing \$96,584.76 in closing funds to be wired to Bank of America account 237037540322, 4002 University Parkway, Winston-Salem, North Carolina. The intended beneficiary was listed as

Michael and Lydia Wysz. Bank of America account 237037540322 lists the account in the name of Different Cloth Cleaning with Clarence McCorkle, DOB June 4, 1990, as the signer for the account. Following the fraudulent wire transfer of \$96,584.76 on 12/07/2017, several transactions occurred on December 8, 2018. These transactions totaled \$76,464.46. On December 8, 2017, a cashier's check made payable to Throne Management Group LLC for James RAGLAND in the amount of \$31,620.00 was obtained at Bank of America, 698 Hanes Mall Boulevard, Winston-Salem, North Carolina. On December 8, 2017, a cashier's check made payable to Throne Management Group LLC for James RAGLAND in the amount of \$34,880.00 was obtained at Bank of America, 1209 Silas Creek Parkway, Winston-Salem, North Carolina. In addition to the cashier's checks, on December 8, 2017, a \$5,000.00 teller withdrawal occurred at Bank of America, 4000 University Parkway, Winston-Salem, North Carolina.

BACKGROUND CONCERNING E-MAIL

15. In general, an e-mail that is sent to a Google Inc. subscriber is stored in the subscriber's "mail box" on Google Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google Inc. servers indefinitely. Even if the

subscriber deletes the e-mail, it may continue to be available on Google Inc.'s servers for a certain period of time.

16. In my training and experience, I have learned that Google Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the public. Google Inc. allows subscribers to obtain e-mail accounts at the domain name @gmail.com, such as the e-mail account[s] listed in Attachment A. Subscribers obtain an account by registering with Google Inc. During the registration process, Google Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google Inc. subscribers) and information concerning subscribers and their use of Google Inc. services, such as account access information, e-mail transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

17. A Google Inc. subscriber can also store with the provider files in addition to e-mails, such as address books, Google Hangouts, contact or buddy lists, calendar data, chat history, pictures via a linked Google Photos account (other than ones attached to e-mails), bookmarks, and other files such as those stored in linked Google Documents and Google Drive

applications, on servers maintained and/or owned by Google Inc. Google Inc. also stores search terms entered into Google Search tool by a user who is simultaneously logged into their Google e-mail account. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures, files, and search terms.

18. In my training and experience, e-mail providers generally ask their subscribers to provide certain personal identifying information when registering for an e-mail account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

19. In my training and experience, e-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the

account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

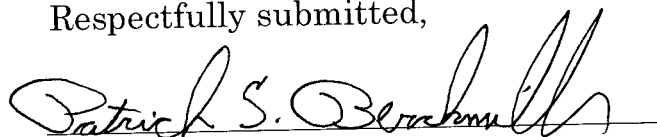
20. In my training and experience, in some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

CONCLUSION

21. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google Inc. who will then compile the requested records at a time convenient to it, there

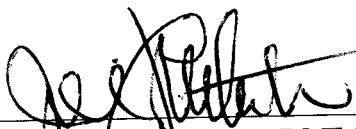
exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Patrick S. Berckmiller
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on 20th Day of November 9:05 AM
2018



THE HONORABLE JOE L. WEBSTER
UNITED STATES MAGISTRATE JUDGE
MIDDLE DISTRICT OF NORTH CAROLINA

ATTACHMENT A

Property to Be Searched

This warrant applies to all information associated with all Google services associated with the account listed below, including but not limited to e-mail, chat communications, search history, contacts, calendar entries, Google Drive documents, Google Hangouts, bookmarks, Google Photo Albums, which are stored at premises controlled by Google Inc., a company that accepts service of legal process at 1600 Amphitheatre Parkway, Mountain View, California, 94043, and electronic legal process via the Google Law Enforcement Response System (LERS) at <https://www.lers.google>:

ashwimvijayrao@gmail.com

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS

RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct.

I am employed by Google Inc., and my official title is

_____. I am a custodian of records for Google Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google Inc., and that I am the custodian of the attached records consisting of _____

(pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google Inc.; and

c. such records were made by Google Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google Inc. (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, in the form of emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A for the time period January 1, 2018 – September 1, 2018:

- a. The contents of all e-mails associated with the account, in the form of stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, originating IP information for all e-mails sent from the account, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used

to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, in the form of address books, contact and buddy lists, calendar data, pictures, search history, Google Chat history, Google Documents files, Google Drive files, bookmarks, Google Photos albums and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of 18 U.S.C. § 1343, Fraud by wire, radio or television, and 18 U.S.C. § 1349, Attempt and conspiracy, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Preparatory steps and communications taken in furtherance of fraud by wire, radio or television, including attempt and conspiracy.

- b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.